Information Security Policy Compliance Systematic Literature Review

by Okfalisa Okafalisa

Submission date: 30-Mar-2020 12:18PM (UTC+0700)
Submission ID: 1285071671
File name: tion_Security_Policy_Compliance_Systematic_Literature_Review.pdf (559.09K)
Word count: 5500
Character count: 32373

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 161 (2019) 1216–1224

Procedia Computer Science

www.elsevier.com/locate/procedia

The Fifth Information Systems International Conference 2019

Information Security Policy Compliance: Systematic Literature Review

Angraini[a,d,*], Rose Alinda Alias[b], Okfalisa[c]

[a]School of Computing, Faculty Engineering, Universiti Teknologi Malaysia, 81310 Johor, Malaysia
[b]Department of Information Systems, Azman Hashim International Business School, Universiti Teknologi Malaysia,81310 Johor Malaysia
[c]Department of Informatic Engineering, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau
[d]Department of Information Systems, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau

Abstract

The growth of research in information technology security has enlarged in recent years. Investigations in Information security besides discussing technical problems but also consider policies, behavior and user compliance issues. Therefore, a systematic review is needed to inform the development of research in compliance with information security policies. This literature review aims to find the challenges and explore the current state-of-the art of information security policy compliance. We identified 305 research papers published on topics of information security policy compliance between 2014 and 2019 and extract 53 documents from discussing with inclusion and exclusion criteria. This literature review found there is lack of study about an evaluation of information security policy compliance using specific metric and need to enhance the model of information security policy compliance with organizational theories.

Keywords: Information security policy; Compliance; Literature review; Evaluation

1. Introduction

Information security policy is a document to ensure information asset and secure technology information with a specific procedure to support the organization objectives [1]. Information security policy ensures information asset

* Corresponding author. Tel.: +62-813-2636-8388.
E-mail address: angraini@uin-suska.ac.id

10.1016/j.procs.2019.11.235

and information technology secure with a specific procedure to support an organization aim and goal. an important issue is management support during implementation of information security policies. When support is obtained, another challenge faced is ensuring that policies are truly able to improve security [2]. Management will be compared to technical products; efficiency of value policies is more difficult to achieve. This is always easier for technical products, because they can often debate efficiency based on statistics. Though organization implemented securities policy still founded employee ignored rule and unexpected behavior. Without compliance, policies are only on the paper on which they are printed or the bits in which they are stored. Compliance with policies aims to ensure the application of organizational security standards [3]. Previous researchers have investigated to formulate the model of user compliance with information security policies. Bulgurcu (2010) investigates rationality-based factors that encourage an employee to comply with ISP requirements concerning protecting information resources and organizational technology and argue that employee attitudes are influencing by compliance benefits, compliance costs, and non-compliance costs, which are beliefs about valuation as consequences of compliance or non-compliance[4] . Users did not realize the importance of compliance with security policy until incidents occur and organizations get impact must incur extra costs due to non-compliance behaviour. Phamz (2015) explores the literature to find out the relevance of user motivation, regulation and user orientation towards information security compliance [5]. Various research has been done to learn about compliance with information security, the majority of research is conducted to find out what factors influence user compliance behavior. There is clearly an insufficiency approach and lack of solutions to improve user compliance behavior with information security policies. There is more information still can be explored to increase understanding of compliance and enhance user compliance with information security policy. Therefore, necessary to conduct a systematic literature review to find trend and challenges from previous research. An effective systematic Literature review requires specific research questions to keep focused. Therefore, this literature review identifies the most significant journals in information security compliance field and found trends and challenges in information security compliance, this paper is structured: section 2 presents the research method used to produce a literature review systematically and discusses the strategies used to look for primary studies and study selection criteria. Section 3 presents the data extracted from the review data that has been carried out in the form of statistics. Section 4 presents an analysis of findings and directives for future research. Finally, Section 5 presents conclusions.

2. Methodology

The literature review procedure used in this study is a systematic literature review. A systematic literature review is a systematic, explicit and comprehensive process to identify, evaluate and synthesise from results of works produced researchers, scholars and practitioners. The literature review process has four stages before writing a review; planning, selection, extraction, and execution [6]. The planning stage is the first stage that will define the purpose of the literature review and protocol that will be carried out to get the literature by the research questions. Then the literature search is done using the keywords and applied to the digital library. It explains the quality of the search results to guarantee the results found before it carries data extraction out. It conducted quantitative and qualitative analyses to analyse the findings and conclusions displayed because of the review. An effective systematic Literature review requires specific research questions to keep focused. Research questions for this literature review explained in Table 1.

Table 1. Research question for the literature review.

ID	Research Question	Aim
RQ 1	Which journal is the most significant journal published information security compliance topic	Identify the most significant journals in information security compliance field
RQ 2	What kinds of trends and challenges in information security compliance field select?	Identify trends and challenges in information security compliance
RQ 3	What kind of theories are used in information security policies compliance?	Identify the trends of theories used in information security policies compliance model

The strategy of literature searching has a significant function in extracting information in the review paper. The stages in the search process consist of determining the database, defining keywords and terms to be searched for, determining search strings, and executing keyword [7]. The database used in this study chosen based on the amount of data and the field of study. List of digital databases used in the search process are: Scopus (www.scopus.com), Web of science (http://apps.webofknowledge.com), ProQuest (www.proquest.com), Springer Link (https://link.springer.com), Jstor (www.jstor.org), IEEE explore (ieeexplore.ieee.org) , ScienceDirect (sciencedirect.com), Emerald insight (https://www.emeraldinsight.com), AIS library (https://aisel.aisnet.org).Searching progress using the strings and combination of keywords include: Information security policy/policies, Compliance/ compliant /Comply/ non-comply, Conformance/ adherence/ obedience, Human security behavior, Organization factors, Evaluation / measure / assessment Searching on databases limited by title, keyword, year, type of publication, and abstract. Searches are limited to publications from 2014 to 2018. The publications used are sourced from the journal article, thesis, and book section and conference proceedings and written in English. After the searching phase, the next phase selected to answer the literature review research question. Criteria for selecting the paper determine and applied in the inclusion and exclusion criteria. Paper selection criteria needed to written explicit because it is helping researchers in deciding and keep on the track during the search process — inclusion and exclusion criteria described in Table 2.

Table 2. Table criteria inclusion and exclusion.

Inclusion criteria	written in English
	time publication at 2014 to 2018
	study discussion about human behavior in information security policies and about organization compliance in area information security, information technology, and management information system
	if similar paper found at a conference and journal, only from the journal will be included
Exclusion criteria	studies without validation and experimental result
	studies from organization report, opinion papers, and editorial
	studies circumstantial about organization culture, compliance and behavior psychology

This research using Mendeley's reference management software (http://mendeley.com) to save search results and gather article. For detailed search process, this research adopts selection process based on PRISMA guidelines. PRISMA is a set of minimum evidence-based items for reporting in systematic reviews and meta-analyses [8]. PRISMA is one method that can be used to report systematic reviews from further research. To simplify create search process, PRISMA provides a generator flow diagram tool (http://prisma.thetacollaborative.ca).The results of the flow diagram from the search process of the article in this study can be seen in Fig. 1.

The article selection process produced 59 articles, which were the primary studies in this study. The criteria used besides those described in the inclusion and exclusion criteria also use quality studies, duplication of several databases used. Also, relevance with the research question and the similarity of studies include to a full-text screening process. Finally, there are found main article will be discussed in this research. The next stage is to extract the data generated from the selection process using file extraction/data encoding standard. The main articles will be extracted to collect data that will contribute to answering the research questions in this review. For each of the 59 main studies selected, only use 52 paper for subsequent analysis, six papers eliminated because of a review paper and one of paper is patent paper. Only research paper with empirical data will be used and the data extraction form has completed. The data extraction form is designed to collect data from the primary studies needed to answer research questions — this research using NVIVO qualitative software to analysis data at systematic literature review [9]. Next process is creating a concept map for support coding process and analysis, from Concept maps can create nodes to explore and describe pattern data. The concept map begins with topic research on information security policy compliance, then nodes are determined according to the purpose of the research question. Therefore, it is necessary to create a node about the problem, objectives, methods, theories used, and discussion from the literature review.

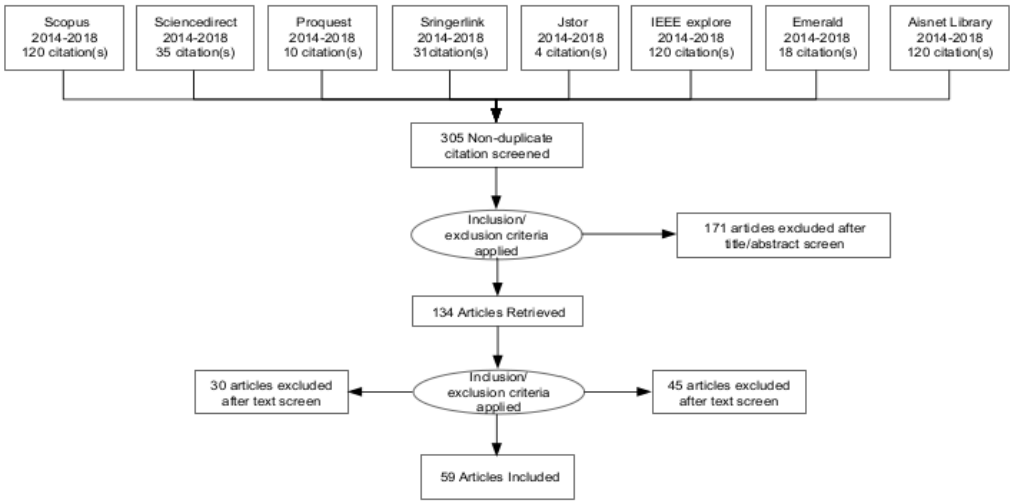

Fig. 1. Flow diagram of article selection.

3. Result and finding

The last stage of the systematic literature review is quantitative and qualitative finding analysis. Findings from the literature review will answer the literature review research question. The results of the literature review on information security policy compliance found 59 articles consisting of 35 journal articles, 22 conference proceeding articles, one book section and one thesis. Compliance with information security policies has become the attention of researchers in the past five years. Therefore, the number of researches at this domain slightly increase during the 2014 – 2018 years. Moreover, there are two paper will be published for forthcoming 2019. This research topic leading with a quantitative approach, of which 59 articles founded, 64% were quantitative, 26% qualitative and 10% used mixed methods. Information and computer security journal is the most significant published journal information security compliance topic. Furthermore, reputable journals such as computer and security, information and management, information system journal, and soft computing journals published some article about this topic and another article published at the annual conference. Based on RQ 1 of a systematic literature review, information and computer security journal is the most important published journal information security compliance topic. For five years, researcher objective is finding influencing factors employee comply with information security policy behaviour intention and measure compliance. The previous study majority study about human behaviour to find factors that influence employees to comply with information security policies. People are often the weakest connection, through cooperation and coordination, they can also be a source of high strength in developing defences that effective and efficient [10]. Fig. 2 describes the trend of a research objective from 2014 to 2019.

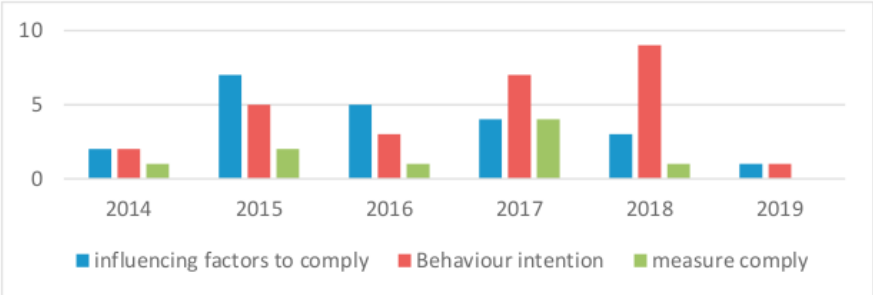

Fig. 2. Research objective trend.

The implementation of an information security policy can be unsuccessful if users do not meet the security requirements. Individual factors (direct or indirect) can impact to behaviour intention to comply with security policies and their overall security behaviour [11]. Therefore, much research conducted to determine the influencing factors of compliance with information security policies and user behaviour intentions to adhere to policies continuously. Research on human behaviour in compliance with information security policies examines factors that cause users to comply with the policies implemented. The results of the literature review, as many as 47% of studies found human factors that influence user behaviour intentions to comply with information security and 38% conducted empirical tests of human behaviour factors that affect compliance with information security policies while only 15% of researchers measure user behaviour. However, there is still a lack of researchers to evaluate compliance with information security policies. This finding answer RQ 2 to identify the trends and challenges in information security compliance. Table 3 describes summary research object from previous research.

Table 3. Research objective from previous study.

Research objective	Author
Behaviour intention	[12, 13. 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35]
Influencing human factors to comply	[19,24,36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55]
Evaluation and measurement information security policy compliance	[41,56, 57, 58, 59, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61]

Measurement of compliance with information security policies cannot use international standards such as ISO 27001 because information security policies developed by organisations differ according to organisational characteristics [62]. IS security research has historically concentrated on evaluating the effects of phenomena on behavioral intentions rather than actual behavior. Merrit (2016) believes that there is a gap between behavioral intentions and actual behavior - especially about compliance with information security policies because many found in previous studies see compliance motivation that will have an impact on behavioral intentions [20]. There are several published studies about human behaviour in information security. This literature review finding 29 theories about human behaviour and 13 organisational theories has been used at information security compliance research. This finding answer RQ 3 to theories are used in information security policies compliance. The theory that widely used is the theory of planned behaviour (TPB). This theory is the fundamental theory of the study of human behaviour. TPB predicts intention-behaviour based on personal attitudes (state of mind), social pressure from others (subjective norms), and a sense of control (perceived behavioural control) [63]. However, behavioural intentions can become active only if the behaviour is in the under volitional control and norms. Abed (2016) state user intention causes to comply with the policy or to refuse [12]. Research use other theories to explore significant human factors to protect information. The next theory commonly used is General Deterrence Theory (GDT). The general deterrence theory used by researchers because it assumes that evaluate preventive behaviour will eliminate information security threats and reduce the risk. The theory of protection motivation theory is considered capable of knowing human behaviour to maintain information security. PMT was first formulated as a comparative theory of fear before it was expanded to a more general theory of persuasive communication[64,65]. This theory argues that two cognitive processes can determine individual intentions to perform protective behaviour, that is, their protective motivation. The study by moody (2018) offers probably the most comprehensive empirical analysis of a model of information security policy compliance with eleven theories [41]. Although using complex theories, Moody's research still does not have a cultural element, so further research may be needed to be able to theorise and examine cultural differences.

4. Discussion

A systematic literature review is a review method that can be used to find and synthesise previous studies. This

method is better than the traditional method because the search process and the process of getting the analysis are structured. The results of the literature review study showed that the amount of research in the field of information security compliance policies is growing. Implementation of Information security policy need will be more successful if the user can full the requirement. From an analysis of the literature review can be found two research GAPs.

1. There is a lack of study about evaluating information security policies compliance.

Internal employee behaviour produces security behaviour that needs to observe and monitored by the organisation to ensure compliance with the applied policy. Periodic and random evaluations must be conducted to ensure compliance. For examples are assessments security awareness and training programs with metrics and produce a percentage of system users who receive basic awareness training, the rate of security personnel in information systems that get security education, and the rate of users with passwords that align with security strategies[66].Security policies must continue to be reviewed and updated regularly by considering changes in circumstances, environment, changing needs in the business context and identified risk. Organizations that develop information security policies based on the needs and types of organizations do not correctly use existing rules on standards or best practices to evaluate their information security policies. This evaluation will cause low ratings because they ignore standards or best practices when developing an information security policy. In the university's context, evaluating compliance with policies will help the organisation know the level of compliance with information technology users. So that, the level of information security threats that come from the behaviour of users who do not care will decrease.

2. Need improvement information security policies compliance model with organisation theories.

Information security behaviour has the opportunity to combine people, technology and organisations. Understanding individual behaviour will enhance positive behaviour while reducing harmful behaviour. Understanding human behaviour will be able to improve adherence to policies by knowing the motivation, modification and prevention [67] and continue investigating can enhance user compliance [12]. Thus, it is necessary to study another factor that affects employee to comply with information security policies. Its support with the significant impact of the organisational variable on the increased effectiveness during implementing information security management [68]. Research on this subject has been mostly restricted to limited comparisons of theory about human behaviour. Therefore, it is necessary to consider human factors and organizational factors to evaluate compliance with information security policies [69,70].

5. Conclusion

This paper found Research GAP from the previous study. First, research on compliance with information security in the majority uses human behavior theory; it needs further study of other factors that can influence compliance with organizational theory. Second, lack of study to evaluating compliance with information security policy. Further research needs to be developed instruments that can be used to measure compliance with information security policies. Therefore, necessary to develop a model from organizational theory and human behavior theory to measure compliance. This model expected can be applied by organizations to improve user compliance and to know the effectiveness of information security policies

References

[1] Doherty, N.F., and H. Fulford H. (2006) "Aligning The Information Security Policy with The Strategic Information Systems Plan." *Comput Secur* **25**: 55–63. doi:10.1016/j.cose.2005.09.009.

[2] Nohlberg, M. (2009) "Why Humans are the Weakest Link." *Soc. Hum. Elem. Inf. Secur. Emerg. Trends*. p. 22.

[3] Barry, L. (2013) *Information Security Policy Development for Compliance*, Boca Raton, CRC Press Taylor & Francis Group.

[4] Bulgurcu, B., H. Cavusoglu, and I. Benbasat. (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Q* **34**: 523–48. doi:10.1093/bja/aeq366.

[5] Phamz, C.H., and M. Nkhoma. (2015) "Security Compliance-New Insight from Goal Orientations and Self-Regulation Theory", in *WMSCI 2015 - 19th World Multi-Conference Syst. Cybern. Informatics, Proc.* **2**.

[6] Okoli, C., and K. Schabram. (2010) "A Guide to Conducting a Systematic Literature Review of Information Systems Research." *Work Pap Inf Syst* **10**: 1–51. doi:10.2139/ssm.1954824.
[7] Bandara, W., S. Miskon, and E. Fielt. (2011) "A Systematic, Tool-Supported Method for Conducting Literature Reviews in IS." *Inf Syst* J. pp. 1–14.
[8] Liberati, A., D.G. Altman, J. Tetzlaff, C. Mulrow, P.C. Gøtzsche, J.P.A. Ioannidis, et al. (2009) "The PRiSMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Healthcare Interventions: Explanation and Elaboration." *BMJ Br Med J.* doi:10.1136/bmj.b2700.
[9] O'Neill, M. M., S.R. Booth, and J.T. Lamb. (2018) "Using NVivo™ for Literature Reviews: The EightStep Pedagogy (N7+1)." *The Qualitative Report* **23 (13)**: 21-39. Available from: https://nsuworks.nova.edu/tqr/vol23/iss13/. [Accessed 12 August 2019].
[10] Safa, N.S., and R. Von Solms. (2016) "An Information Security Knowledge Sharing Model in Organizations." *Comput Human Behav* **57**: 442–51. doi:10.1016/j.chb.2015.12.037.
[11] Consolvo, S., and M. Langheinrich. (2015) "Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance." *Priv. Secur. ACM SIGCAS Comput. Soc.* **31**: 8–23. doi:10.1145/503345.503347.
[12] Abed, J., G. Dhillon, and S. Ozkan. (2016) "Investigating Continuous Security Compliance Behavior : Insights from Information Systems Continuance Model", in *Twenty-second Am. Conf. Inf. Syst. San Diego*. p. 1–10.
[13] Alzahrani, A., C. Johnson, and S. Altamimi S. (2018) "Information Security Policy Compliance : Investigating the Role of Intrinsic Motivation Towards Policy Compliance in The Organisation", in 2018 *4th Int. Conf. Inf. Manag., IEEE*. p. 125–32. doi:10.1109/INFOMAN.2018.8392822.
[14] Hwang, I., D. Kim, T. Kim, and S. Kim. (2017) "Why not Comply With Information Security? An Empirical Approach for The Causes of Non-Compliance." *Online Inf Rev* **41**: 2–18. doi:10.1108/OIR-11-2015-0358.
[15] Ifinedo, P. (2014) "Information Systems Security Policy Compliance: An Empirical Study of The Effects of Socialisation, Influence, and Cognition." *Inf Manag* **51**: 69–79. doi:10.1016/j.im.2013.10.001.
[16] Kajtazi, M., B. Bulgurcu, H. Cavusoglu, and I. Benbasat. (2014) "Assessing Sunk Cost Effect on Employees' Intentions to Violate Information Security Policies in Organizations", in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.* pp. 3169–77. doi:10.1109/HICSS.2014.393.
[17] Kajtazi, M., H. Cavusoglu, I. Benbasat, and D. Haftor. (2018) "Escalation of Commitment as an Antecedent to Noncompliance with Information Security Policy." *Inf Comput Secur* **26**: 171–93. doi:10.1108/ICS-09-2017-0066.
[18] Kim, H.L., and J. Han. (2018) "Do Employees in A "Good" Company Comply Better With Information Security Policy? A Corporate Social Responsibility Perspective." *Inf Technol People*. ITP-09-2017-0298. doi:10.1108/ITP-09-2017-0298.
[19] Lowry, P.B., and G.D. Moody. (2015) "Proposing The Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies." *Inf Syst J* **25**: 433–63. doi:10.1111/isj.12043.
[20] Merritt, C.D., and G.S. Dhillon. (2016) "What Interrupts Intention to Comply with IS- Security Policy ?" *Twenty-second Am. Conf. Inf. Syst.* p. 1–10.
[21] Nasir, A., R.A. Arshah, and M.R. Ab Hamid. (2017) "Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture", in *Proc. 2017 Int. Conf. Inf. Syst. Data Min. - ICISDM* '17. p. 56–60. doi:10.1145/3077584.3077593.
[22] Rajab, M., and A. Eydgahi. (2019) "Evaluating The Explanatory Power of Theoretical Frameworks on Intention to Comply with Information Security Policies in Higher Education." *Comput Secur* **80**: 211–23. doi:10.1016/j.cose.2018.09.016.
[23] Siponen, M., M. Adam Mahmood, and S. Pahnila. (2014) "Employees' Adherence to Information Security Policies: An Exploratory Field Study." *Inf Manag* **51**: 217–24. doi:10.1016/j.im.2013.08.006.
[24] Amankwa, E., M. Loock, and E. Kritzinger. (2018) "Establishing Information Security Policy Compliance Culture in Organizations." *Inf Comput Secur* **26**: 420–36. doi:10.1108/ICS-09-2017-0063.
[25] Sommestad, T., H. Karlzén, and J. Hallberg. (2015) "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour." *Int J Inf Secur Priv* **9**: 26–46. doi:10.4018/IJISP.2015010102.
[26] Stewart, H., and J. Jürjens. (2017) "Information Security Management and The Human Aspect in Organizations." **5**. doi:10.1108/ICS-07-2016-0054.
[27] Yakimin, Y., and G. Dhillon. (2015) "Employee ISP Compliance Intentions : An Empirical Test of Empowerment Employee", in *Thirty Sixth Int. Conf. Inf. Syst.* p. 1–26.
[28] Yazdanmehr, A., and J. Wang. (2016) "Employees' Information Security Policy Compliance : A Norm Activation Perspective." *Decis Support Syst* **92**: 36–46. doi:10.1016/j.dss.2016.09.009.
[29] Aurigemma, S., and T. Mattson. (2017) "Privilege or Procedure: Evaluating The Effect of Employee Status on Intent to Comply with Socially Interactive Information Security Threats and Controls." *Comput Secur* **66**: 218–34. doi:10.1016/j.cose.2017.02.006.
[30] Aurigemma, S. and T. Mattson. (2017) "Deterrence and Punishment Experience Impacts on ISP Compliance Attitudes." *Inf Comput Secur* **25**: 421–36. doi:10.1108/ICS-11-2016-0089.
[31] Bauer, S., E.W.N Bernroider, and K. Chudzikowski. (2017) "Prevention is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-Compliance with Information Security Policies in Banks." *Comput Secur* **68**: 145–59. doi:10.1016/j.cose.2017.04.009.
[32] Doherty, N.F., and S.T. Tajuddin. (2018) "Towards a User-Centric Theory of Value-Driven Information Security Compliance." *Inf Technol People* **31**: 348–67. doi:10.1108/ITP-08-2016-0194.
[33] Garz. V. (2015) "Securing BYOD : A Study of Framing and Neutralization Effects on Mobile Device Security Policy Compliance", in *Proc. 36th Int. Conf. Inf. Syst.* p. 1–10.

[34] Han, J.Y., Y.J. Kim, and H. Kim. (2017) "An Integrative Model of Information Security Policy Compliance with Psychological Contract: Examining a Bilateral Perspective." *Comput Secur* **66**: 52–65. doi:10.1016/j.cose.2016.12.016.
[35] Humaidi, N., and V. Balakrishnan. (2015) "The Moderating Effect of Working Experience on Health Information System Security Policies Compliance Behaviour." *Malaysian J Comput Sci* **28**: 70–92.
[36] Alalwan, JA. (2018) "Fear of Cybercrime and the Compliance with Information Security Policies : A Theoretical Study", in *IC4E 2018*. p. 85–7. doi:10.1145/3183586.3183590.
[37] Hina, S., and D.D. Dominic. (2016) "Information Security Policies: Investigation of Compliance in Universities", in *the 3rd Int. Conf. Comput. Inf. Sci. ICCOINS 2016 - Proc., 2016*. p. 564–9. doi:10.1109/ICCOINS.2016.7783277.
[38] Huang, H., N. Parolia, and K-T. Cheng. (2016) "Willingness and Ability to Perform Information Security Compliance Behavior: Psychological Ownership and Self-Efficacy Perspective", in *Pacific Asia Conf. Inf. Syst*. doi:10.1186/1471-2334-12-S1-O4.
[39] Maphanga, G.C., and O. Jokonya. (2017) "The Risk of Users' Negative Behaviours on Information Security Compliance Policy in Organizations." *Risk Gov Control Financ Mark Institutions* **7**: 30–40. doi:10.22495/rgc7i4art4.
[40] Merhi, M.I., and J. Leighton. (2015) "Top Management Can Lower Resistance toward Information Security Compliance", in *Thirty Sixth Int. Conf. Inf. Syst.* p. 1–11.
[41] Moody, G.D., M. Siponen, and S. Pahnila. (2018) "Toward a Unified Model of Information Security Policy Compliance." *MIS Q* **42**: 285–311. doi:10.25300/MISQ/2018/13853.
[42] Park, M., and S. Chai. (2018) "Internalization of Information Security Policy and Information Security Practice: A Comparison with Compliance", in *Proc. 51st Hawaii Int. Conf. Syst. Sci.* **9**: 4723–31. doi:10.24251/HICSS.2018.595.
[43] Razilan, M., A. Kadir, S. Norwahidah, S. Norman, S.A. Rahman, and A. Bunawan. (2017) "Information Security Policies Compliance among Employees in Cybersecurity Khalid S . Soliman International Business Information Management Association (IBIMA)", in *Proc. 28th Int. Bus. Inf. Manag. Assoc. Conf.*
[44] Sharma, S, and M. Warkentin. (2018) "Do I Really Belong?: Impact of Employment Status on Information Security Policy Compliance." *Comput Secur*. doi:10.1016/j.cose.2018.09.005.
[45] Sikolia, D., D. Twitchell, and G. Sagers. (2016) "Employees' Adherence to Information Security Policies: A Partial Replication", in *Proc. Am. Conf. Inf. Syst.* p. 1–9. doi:10.1109/ICMTMA.2009.433.
[46] Sillic, M. (2019) "Critical Impact of Organizational and Individual Inertia in Explaining Non-Compliant Security Behavior in The Shadow IT Context." *Comput Secur* **80**: 108–19. doi:10.1016/j.cose.2018.09.012.
[47] Talib, Y.Y.A. (2015) *Intrinsic Motivation and Information Systems Security Policy Compliance in Organizations*.
[48] Tsohou, A. and P. Holtkamp. (2018) "Are Users Competent to Comply with Information Security Policies? An Analysis of Professional Competence Models." *Inf Technol People* **31**: 1047–68. doi:10.1108/ITP-02-2017-0052.
[49] Alshare, K.A., P.L. Lane, and M.R. Lane. "Information Security Policy Compliance: A Higher Education Case Study." *Inf Comput Secur* **26**: 91–108. doi:10.1108/ICS-09-2016-0073.
[50] Arage, T., F. Belanger, and T. Beshah. (2015) "Influence of National Culture on Employees' Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies", in *AMCIS 2015 Proc.* p. 1–7.
[51] Bansal, G., and S.I. Shin. (2016) "Interaction Effect of Gender and Neutralization Techniques on Information Security Policy Compliance: An Ethical Perspective", in *AMCIS 2016 Surfing IT Innov. Wave - 22nd Am. Conf. Inf. Syst.* p. 1–10.
[52] Chen, X., D. Wu, L. Chen, and J.K.L. Teng. (2018) "Information & Management Sanction Severity and Employees ' Information Security Policy Compliance : Investigating Mediating, Moderating, and Control Variables." *Inf Manag* **55**: 1049–60. doi:10.1016/j.im.2018.05.011.
[53] Choi, M., and J. Song. (2018) "Social Control Through Deterrence on The Compliance with Information Security Policy." *Soft Comput* **22**: 6765–72. doi:10.1007/s00500-018-3354-z.
[54] Chulkov, D.V. (2017) "Escalation of Commitment and Information Security: Theories and Implications." *Inf Comput Secur* **25**: 580–92. doi:10.1108/ICS-02-2016-0015.
[55] D'Arcy, J., and P.B. Lowry. (2017) "Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study." *Inf Syst J*. pp. 1–27. doi:10.1111/isj.12173.
[56] Alkhurayyif, Y., and G.R.S Weir. (2017) "Readability as a Basis for Information Security Policy Assessment", in *2017 Seventh Int. Conf. Emerg. Secur. Technol.* p. 114–21. doi:10.1109/EST.2017.8090409.
[57] Jin, J., L. Ouyang, and X. Gu. (2015) "Using Galois Lattice to Represent and Analyze Information Security Policy Compliance." *Int Asia Conf Ind Eng Manag Innov* **1**: 239–43. doi:10.2991/978-94-6239-100-0.
[58] Karlsson, F., M. Karlsson, and J. Åström. (2017) "Measuring Employees' Compliance - The Importance of Value Pluralism." *Inf Comput Secur* **25**: 279–99. doi:10.1108/ICS-11-2016-0084.
[59] Kurowski, S. (2018) "Measuring Compliance with Specific Policy Contents - The SRPC- and SRPCC-Scales for a More Detailed Measurement of Positive Policy Compliance", in *Twenty-Sixth Eur. Conf. Inf. Syst.*
[60] Ross, R.S. (2014) "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans." *NIST Spec* Publ. pp. 1–487. doi:10.6028/NIST.SP.800-53Ar4.
[61] Buthelezi, M.P., J.A.Van Der Poll, and E.O. Ochola. (2017) "Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis", in *Proc. - 2016 Int. Conf. Comput. Sci. Comput. Intell. CSCI* 2016. pp. 1360–7. doi:10.1109/CSCI.2016.0254.
[62] Calder, A., and S. Watkins. (2008) *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO27002*.
[63] Ajzen, I. (1991) "The Theory of Planned Behavior." *Organ Behav Hum Decis Process*. doi:10.1016/0749-5978(91)90020-T.
[64] Rogers, R.W. (1975) "A Protection Motivation Theory of Fear Appeals and Attitude Change." *J Psychol*. doi:10.1080/00223980.1975.9915803.

[65] Maddux, J.E., and R.W. Rogers. (1983) "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change." *J Exp Soc Psychol*. doi:10.1016/0022-1031(83)90023-9.
[66] Knapp, K.J., R.F. Morris, T.E. Marshall, and T. Anthony. (2009) "Information Security Policy : An Organizational-Level Process Model." *Comput Secur* **28**: 493–508. doi:10.1016/j.cose.2009.07.001.
[67] Crossler, R.E., A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. (2013) "Future Directions for Behavioral Information Security Research." *Comput Secur* **32**: 90–101. doi:10.1016/j.cose.2012.09.010.
[68] Chang, SE. (2006) "Organizational Factors to The Effectiveness of Implementing Information Security Management." **106**. 2006.
[69] Chang, A.J.T, C.Y. Wu, and H.W. Liu. (2012) "The Effects of Job Satisfaction and Organization Commitment on Information Security Policy Adoption and Compliance", in *2012 IEEE 6th Int. Conf. Manag. Innov. Technol. ICMIT*. pp. 442–6. doi:10.1109/ICMIT.2012.6225846.
[70] Alotaibi, M., S. Furnell, and N. Clarke. (2016) "Information Security Policies : A Review of Challenges and Influencing Factors." pp. 352–8.

Information Security Policy Compliance Systematic Literature Review

ORIGINALITY REPORT

20%	13%	17%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jyx.jyu.fi Internet Source	4%
2	romisatriawahono.net Internet Source	2%
3	Silmie Vidiya Fani, Apol Pribadi Subriadi. "Business Continuity Plan: Examining of Multi-Usable Framework", Procedia Computer Science, 2019 Publication	1%
4	thescipub.com Internet Source	1%
5	Salvatore Aurigemma, Thomas Mattson. "Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls", Computers & Security, 2017 Publication	1%
6	creativecommons.org Internet Source	1%
7	pearl.plymouth.ac.uk	

	Internet Source	1%
8	onlinelibrary.wiley.com Internet Source	<1%
9	bmchealthservres.biomedcentral.com Internet Source	<1%
10	Betty Purwandari, Mochammad Arief Hermawan Sutoyo, Muhammad Mishbah, Muhammad Fadhil Dzulfikar. "Gamification in e-Govemment: A Systematic Literature Review", 2019 Fourth International Conference on Informatics and Computing (ICIC), 2019 Publication	<1%
11	Iden, Jon, and Tom Roar Eikebrokk. "Implementing IT Service Management: A systematic literature review", International Journal of Information Management, 2013. Publication	<1%
12	Mutlaq Alotaibi, Steven Furnell, Nathan Clarke. "Information security policies: A review of challenges and influencing factors", 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016 Publication	<1%
13	Majed Rajab, Ali Eydgahi. "Evaluating the explanatory power of theoretical frameworks	<1%

on intention to comply with information security policies in higher education", Computers & Security, 2019
Publication

14	Princely Ifinedo. "Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions", Information Resources Management Journal, 2018 Publication	<1%
15	Fredrik Karlsson, Martin Karlsson, Joachim Åström. "Measuring employees' compliance – the importance of value pluralism", Information and Computer Security, 2017 Publication	<1%
16	docsdrive.com Internet Source	<1%
17	scholarworks.waldenu.edu Internet Source	<1%
18	Joseph Birundu Mogendi, Hans De Steur, Xavier Gellynck, Anselimo Makokha. "A novel framework for analysing stakeholder interest in healthy foods: A case study on iodine biofortification", Ecology of Food and Nutrition, 2016 Publication	<1%
19	pdfs.semanticscholar.org Internet Source	<1%

20	Nader Sohrabi Safa, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, Tutut Herawan. "Information security conscious care behaviour formation in organizations", Computers & Security, 2015 Publication	<1%
21	Harry Prapavessis, Ralph Maddison, Peter N Ruygrok, Sandra Bassett, Therese Harper, Lisa Gillanders. "Using Theory of Planned Behavior to understand exercise motivation in patients with congenital heart disease", Psychology, Health & Medicine, 2005 Publication	<1%
22	Adéle Da Veiga. "Comparing the information security culture of employees who had read the information security policy and those who had not", Information and Computer Security, 2016 Publication	<1%
23	Antoni Lluís Mesquida, Antonia Mas. "Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension", Computers & Security, 2015 Publication	<1%
24	Sang Soo Kim, Yong Jin Kim. "The effect of compliance knowledge and compliance support systems on information security compliance behavior", Journal of Knowledge	<1%

Management, 2017
Publication

25	www.tandfonline.com Internet Source	<1%
26	people.utm.my Internet Source	<1%
27	studentsrepo.um.edu.my Internet Source	<1%
28	azhin.org Internet Source	<1%
29	Indre Bardauskaite. "Loyalty in the Business-to-Business Service Context: A Literature Review and Proposed Framework", Journal of Relationship Marketing, 2014 Publication	<1%
30	Marie Karim Aboujaoude, Khalil Feghali, Charbel Kfouri. "Chapter 2 Planning the Research", Springer Science and Business Media LLC, 2018 Publication	<1%
31	Sari Agustin Wulandari, Anggi Permata Dewi, M. Rizki Pohan, Dana Indra Sensuse, M. Mishbah, Syamsudin. "Risk Assessment and Recommendation Strategy Based on COBIT 5 for Risk: Case Study SIKN JIKN Helpdesk Service", Procedia Computer Science, 2019 Publication	<1%

dspace.lboro.ac.uk

32	Internet Source	<1%
33	Adéle da Veiga, Liudmila V. Astakhova, Adéle Botha, Marlien Herselman. "Defining organisational information security culture—Perspectives from academia and industry", Computers & Security, 2020 Publication	<1%
34	www.koreascience.or.kr Internet Source	<1%
35	"Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D", Springer Science and Business Media LLC, 2019 Publication	<1%
36	repository.tudelft.nl Internet Source	<1%
37	www.emeraldinsight.com Internet Source	<1%
38	www.ukessays.com Internet Source	<1%
39	Yousef Mohammad Iriqat, Abd Rahman Ahlan, Nurul Nuha Abdul Molok. "Information Security Policy Perceived Compliance Among Staff in Palestine universities: An Empirical Pilot study", 2019 IEEE Jordan International	<1%

Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019
Publication

---

40 Joseph Omidosu, Jacques Ophoff. "A theory-based review of information security behavior in the organization and home context", 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), 2016 <1%
Publication

---

41 Yuxiang Hong, Steven Furnell. "Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization", Journal of Computer Information Systems, 2019 <1%
Publication

---

42 Neil F. Doherty, Heather Fulford. "chapter 3 Exploring the Effectiveness of Information Security Policies", IGI Global, 2007 <1%
Publication

---

43 Martin (Dae Youp) Kang, Anat Hovav. "Benchmarking Methodology for Information Security Policy (BMISP): Artifact Development and Evaluation", Information Systems Frontiers, 2018 <1%
Publication

---

44 Mark Evans, Ying He, Cunjin Luo, Iryna Yevseyeva, Helge Janicke, Leandros A. Maglaras. "Employee Perspective on <1%

Information Security Related Human Error in Healthcare: Proactive Use of IS-CHEC in Questionnaire Form", IEEE Access, 2019
Publication

45 Suresh Cuganesan, Cara Steele, Alison Hart. "How senior management and workplace norms influence information security attitudes and self-efficacy", Behaviour & Information Technology, 2017 <1%
Publication

46 Heredia, Alberto, Ricardo Colomo-Palacios, and Antonio de Amescua. "Software Business Models from a Distribution Perspective: A Systematic Mapping Study", Procedia Computer Science, 2015. <1%
Publication

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		